UPDATE ON THE CERN COMPUTING AND NETWORK INFRASTRUCTURE FOR CONTROLS (CNIC)

S. Lüders on behalf of the CNIC WG

CERN IT/CO, Geneva, Switzerland

ABSTRACT Over the last few years modern accelerator and experiment control systems have increasingly been based on commercial-off-the-shelf products (VME crates, PLCs, SCADA systems, etc.), on Windows or Linux PCs, and on communication infrastructures using Ethernet and TCP/IP. Despite the benefits coming with this (r)evolution, new vulnerabilities are inherited too: Worms and viruses spread within seconds via the Ethernet cable, and attackers are becoming interested in control systems. Unfortunately, control PCs cannot be patched as fast as office PCs. Even worse, vulnerability scans at CERN using standard IT tools have shown that commercial automation systems lack fundamental security precautions: Some systems crashed during the scan, others could easily be stopped or their process data be altered [1]. During the two years following the presentation of the CNIC Security Policy at ICALEPCS2005 [2], a “Defense-in-Depth” approach has been applied to protect CERN’s control systems. This presentation will give a review of its thorough implementation and its deployment. Particularly, measures to secure the controls network and tools for user-driven management of Windows and Linux control PCs will be discussed.

The (R)Evolution of Control Systems

Controls networks meet campus / business networks

- ► Proprietary field busses (PROFIBUS, ModBus) replaced by Ethernet & TCP/IP (PROFINET, ModBus/TCP)
- ► Field devices connect directly to Ethernet & TCP/IP
- ► Real time applications based on TCP/IP

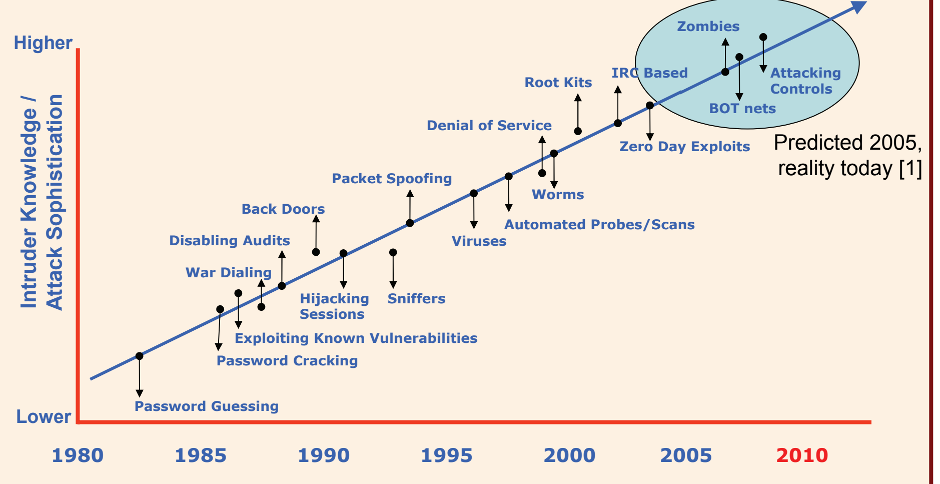
Migration to the Microsoft Windows platform

- ► MS Windows not designed for industrial / control systems
- ► OPC/DCOM runs on port 135 (heavily used for RPC)
- ► STEP7, PL7 Pro, UNITY, WINCC, VNC, PCAnywhere, …

Use of IT protocols & gadgets

- ► eMails, FTP, Telnet, SNMP, HTTP (WWW), … directly on e.g. a PLC
- ► Wireless LAN, notebooks, USB sticks, webcams, …

Control Systems under Attack !?



Predicted 2005, reality today [1]

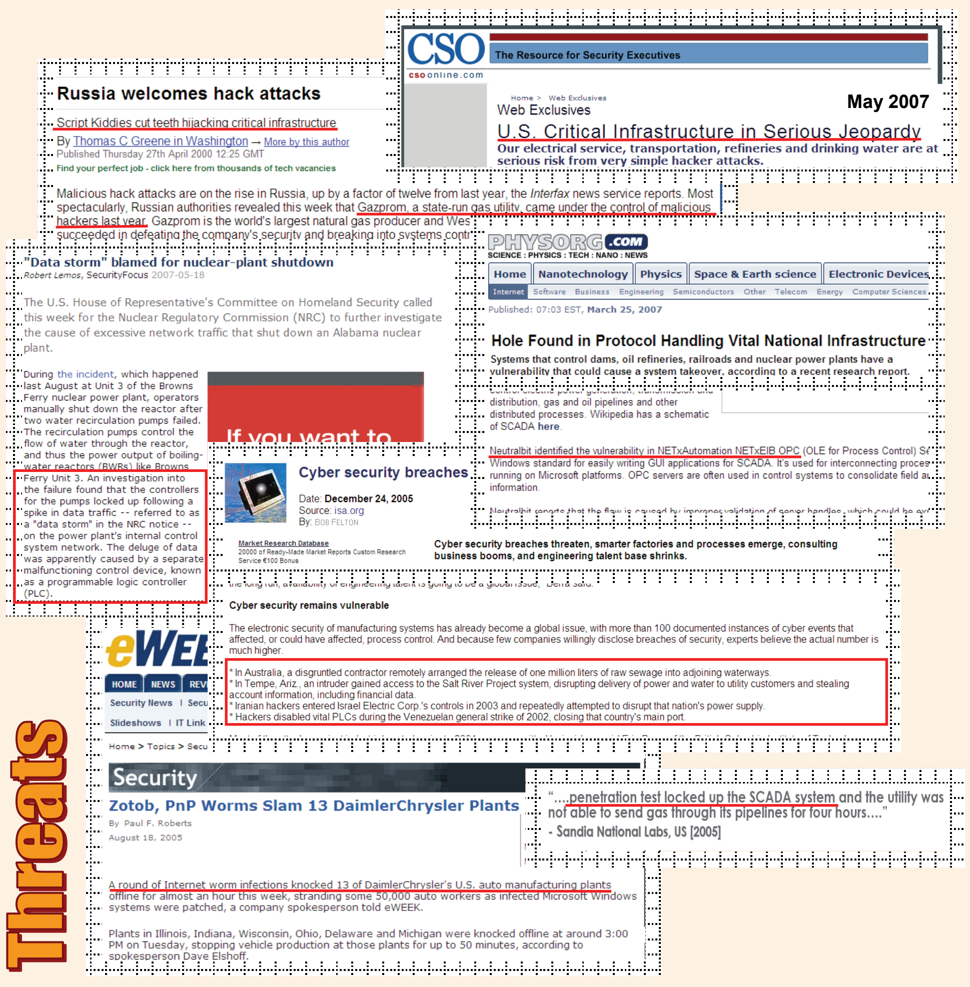
Control Systems: Era of Legacy Technology (“Security through Obscurity”)

Transition Phase (“Controls goes IT”)

Era of Modern Information Technology (“From Top-Floor to Shop-Floor”)

Risk = Threat × Vulnerability × Consequence

Threats



CSO The Resource for Security Executives
csoonline.com
Home > Web Exclusives
Web Exclusives
May 2007
U.S. Critical Infrastructure in Serious Jeopardy
Our electrical service, transportation, refineries and drinking water are at serious risk from very simple hacker attacks.

Russia welcomes hack attacks
Script Kiddies cut teeth hijacking critical infrastructure
By Thomas C Greene in Washington → More by this author
Published Thursday 27th April 2000 12:25 GMT
Find your perfect job - click here from thousands of tech vacancies

Malicious hack attacks are on the rise in Russia, up by a factor of twelve from last year, the *Interfax* news service reports. Most spectacularly, Russian authorities revealed this week that Gazprom, a state-run gas utility, came under the control of malicious hackers last year. Gazprom is the world's largest natural gas producer and Wes succeeded in defeating the company's security and breaking into systems contr

"Data storm" blamed for nuclear-plant shutdown
Robert Lemos, SecurityFocus 2007-05-18

The U.S. House of Representative's Committee on Homeland Security called this week for the Nuclear Regulatory Commission (NRC) to further investigate the cause of excessive network traffic that shut down an Alabama nuclear plant.

During the incident, which happened last August at Unit 3 of the Browns Ferry nuclear power plant, operators manually shut down the reactor after two water recirculation pumps failed. The recirculation pumps control the flow of water through the reactor, and thus the power output of boiling-water reactors (BWRs) like Browns Ferry Unit 3. An investigation into the failure found that the controllers for the pumps locked up following a spike in data traffic -- referred to as a "data storm" in the NRC notice -- on the power plant's internal control system network. The deluge of data was apparently caused by a separate malfunctioning control device, known as a programmable logic controller (PLC).

PHYSORG.COM
SCIENCE : PHYSICS : TECH : NANO : NEWS
Home | Nanotechnology | Physics | Space & Earth science | Electronic Devices
Internet Software Business Engineering Semiconductors Other Telecom Energy Computer Sciences
Published: 07:03 EST, March 25, 2007

Hole Found in Protocol Handling Vital National Infrastructure
Systems that control dams, oil refineries, railroads and nuclear power plants have a vulnerability that could cause a system takeover, according to a recent research report.

distribution, gas and oil pipelines and other distributed processes. Wikipedia has a schematic of SCADA here.

Neutralbit identified the vulnerability in NETxAutomation NETxEIB OPC (OLE for Process Control) Se Windows standard for easily writing GUI applications for SCADA. It's used for interconnecting proces running on Microsoft platforms. OPC servers are often used in control systems to consolidate field a information.

If you want to

Cyber security breaches
Date: December 24, 2005
Source: isa.org
By: Bob Felton

Market Research Database
20000 of Ready-Made Market Reports Custom Research Service €100 Bonus

Cyber security breaches threaten, smarter factories and processes emerge, consulting business booms, and engineering talent base shrinks.

Cyber security remains vulnerable

The electronic security of manufacturing systems has already become a global issue, with more than 100 documented instances of cyber events that affected, or could have affected, process control. And because few companies willingly disclose breaches of security, experts believe the actual number is much higher.

* In Australia, a disgruntled contractor remotely arranged the release of one million liters of raw sewage into adjoining waterways.
* In Tempe, Ariz., an intruder gained access to the Salt River Project system, disrupting delivery of power and water to utility customers and stealing account information, including financial data.
* Iranian hackers entered Israel Electric Corp.'s controls in 2003 and repeatedly attempted to disrupt that nation's power supply.
* Hackers disabled vital PLCs during the Venezuelan general strike of 2002, closing that country's main port.

eWEEK
HOME NEWS REV
Security News | Secu
Slideshows | IT Link
Home > Topics > Secu
Security
Zotob, PnP Worms Slam 13 DaimlerChrysler Plants
By Paul F. Roberts
August 18, 2005

A round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. auto manufacturing plants offline for almost an hour this week, stranding some 50,000 auto workers as infected Microsoft Windows systems were patched, a company spokesperson told eWEEK.

Plants in Illinois, Indiana, Wisconsin, Ohio, Delaware and Michigan were knocked offline at around 3:00 PM on Tuesday, stopping vehicle production at those plants for up to 50 minutes, according to spokesperson Dave Elshoff.

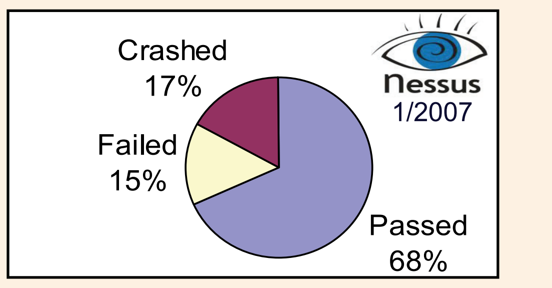
“….penetration test locked up the SCADA system and the utility was not able to send gas through its pipelines for four hours….”
- Sandia National Labs, US [2005]

Vulnerability

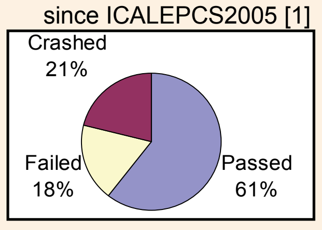
CERN TOCSSiC Vulnerability Scans [1]

31 devices from 7 different manufacturers (53 tests in total)

All devices fully configured <u>but running idle</u>



Situation improved a bit since ICALEPCS2005 [1]



Consequence

***Equipment* being affected or even destroyed**

- ► Some very expensive, esp. in experiments & accelerators
- ► Sometimes impossible to repair / replace

***Processes* being disturbed**

- ► High interconnectivity, thus very sensitive to disturbances
  - *A cooling process PLC failure can stop the accelerator*
  - *A power controller failure can stop a (sub-)detector*
- ► Difficult to configure

***Time* being wasted**

- ► Downtime reduces efficiency (esp. data loss in experiments)
- ► Time needed to re-install, re-configure, test and/or re-start
- ► Requires many people working, possibly outside working hours

CERN's Mitigation: "Defense-in-Depth"

“Defense-in-Depth” means security on *each* layer:

…of the security of the device itself, …of the firmware and operating system, …of the network connections & protocols, …of the software applications (for PLC programming, SCADA, etc.), …of third party software, and …together with users, developers & operators.

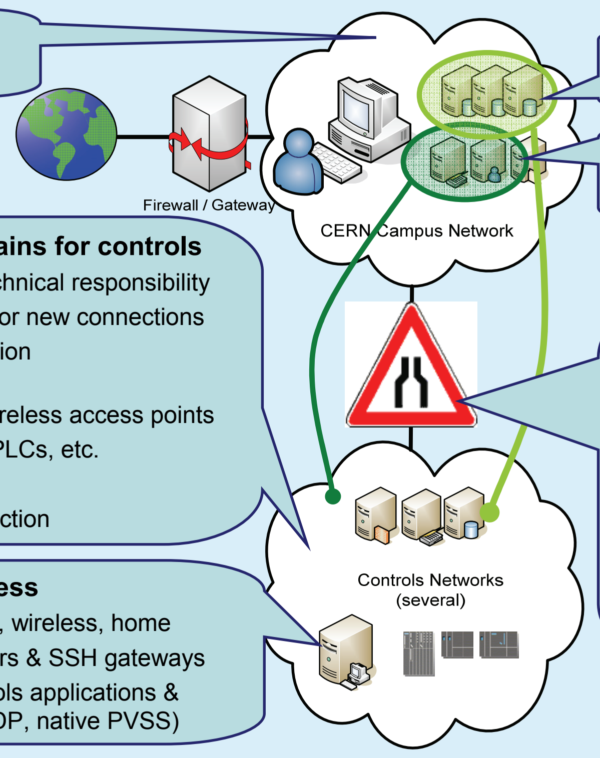
CERN’s solution is based on the “Good Practice Guidelines Parts 1-7” of the U.K. Centre for the Protection of the National Infrastructure (CPNI) [3].

Network Segregation

Campus network for desktop computing

“Fat-Pipe” data transfer to “the GRID”

Essential services are “trusted”:
► DNS, NTP, Oracle, data storage, …



Separate Network Domains for controls

- ► Domain Manager with technical responsibility
- ► Authorization procedure for new connections
- ► MAC address authentication
- ► Only operational devices, but neither laptops nor wireless access points
- ► Additional protection for PLCs, etc.
- ► Network monitoring
- ► Statistics & intrusion detection

Restricted and controlled inter-communication

- ► Traffic filtering (based on ACLs)
- ► Application gateways plus DMZ
- ► Interactive access to the “outside”: Restricted web-browsing, no e-mailing
- ► Only automatic, outgoing e-mails
- ► Rules for file transfers
- ► Disconnection point if threat for others

Remote interactive access

- ► From “outside”, i.e. office, wireless, home
- ► Windows Terminal Servers & SSH gateways
- ► Methods to access controls applications & control PCs (i.e. SSH, RDP, native PVSS)

Central Installation Schemes

From experience at CERN, only centrally managed and patched PCs have shown to be secure in the long run.

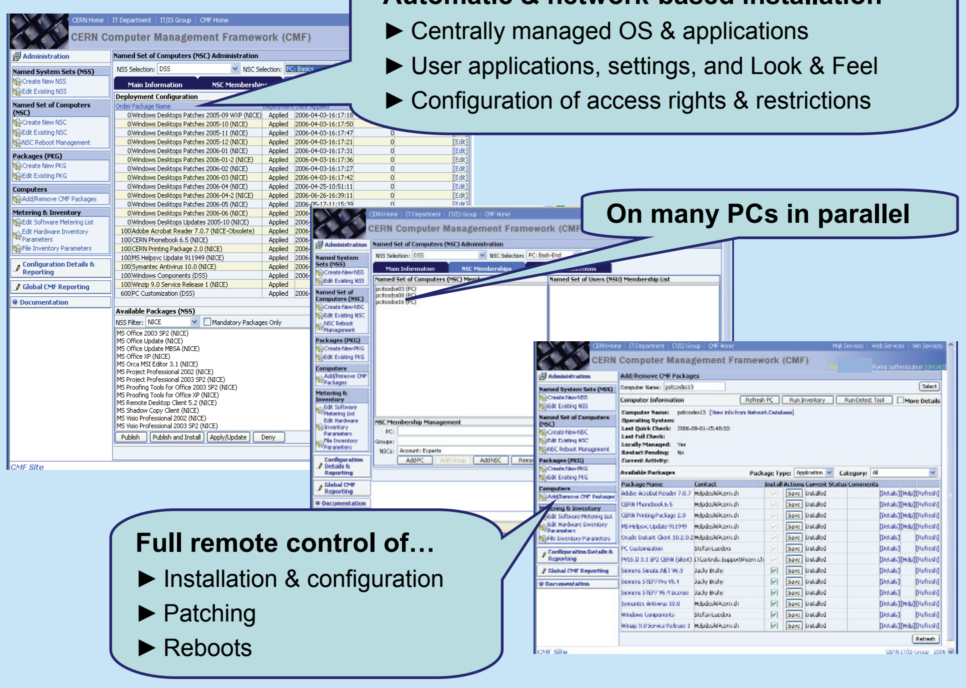
- ► Use centrally managed systems wherever possible
- ► Ensure prompt security updates: OS, applications, anti-virus, etc.

Development of a User-driven PC management

- ► Pass *flexibility* and *responsibility* to the User
- ► *HE* decides *WHEN* to install *WHAT* on *WHICH* control PCs (instead of the IT people)
- ► IT will send out email notifications of new patches to be installed
- ► *HE* has to ensure security
- ► PCs might be blocked if threat for others

Web-based **Computer Management Framework** (CMF) for Window XP and Windows Server [4]

Template-based **Linux For Controls** (L4C) for CERN Scientific Linux 3/4 using quattor



CERN Computer Management Framework (CMF)

Automatic & network-based installation

- ► Centrally managed OS & applications
- ► User applications, settings, and Look & Feel
- ► Configuration of access rights & restrictions

On many PCs in parallel

Full remote control of…

- ► Installation & configuration
- ► Patching
- ► Reboots

… this works even for oscilloscopes !!!

Authentication & Authorization

People are always the weakest link.

- ► Need for a proper, coherent, and CERN-wide access control
- ► Ensuring traceability of access (who, when, and from where)
- ► Passwords must be kept secret: beware of “Google Hacking”
- ► In exceptional cases using strong authentication

Implementation of “Role Based Access Control”

- ► User credentials for authentication
- ► Role assignment for authorization
- ► Strict rules for remote access
- ► Posters by P. Chochula, S. Gysin, K. Kostro, A. Petrov [5]

Still problematic areas: e.g. problems controlling user privileges in commercial controls applications, no generalization to one common central scheme at CERN, lack of access control in standard communication protocols

User Training

Making security an objective

- ► Security training for users, operators, and system experts
- ► Bringing together IT and controls people
- ► Management buy-in due to incident at CERN’s magnet test-stand
- ► Manufacturers and vendors became part of the solution. Security demands will be soon included into orders and call for tenders

Discussion with governments, industry, and users

- ► Control System Cyber-Security (CS^2/HEP) workshop [6]
- ► CERN is chairing the EuroSCSIE, with members from European governments, industry and research institutions that are dependent upon and, or whose responsibility it is to improve the security of SCADA and Control Systems.

Incident Handling & System Recovery

Even with a stringent Security Policy incidents can never be prevented completely.

- ► Incident handling became part of CERN’s general procedures
- ► Handling incidents on a Domain have been and will be jointly performed by CERN’s Computer Security Team and the corresponding Domain Administrator
- ► The acting Computer Security Officer has the right to take appropriate actions in justified emergency cases
- ► CERN’s Central Installation Schemes CMF and L4C allow for prompt system recovery

Auditing & Assessment

Keeping and raising the level of security

- ► Annual reviews of the CNIC Security Policy and its implementation planned for the future; the last being held in summer 2007

SUMMARY Due to the continuing integration of common IT technology into control systems, the corresponding IT security vulnerabilities and cyber-attackers end up threatening control systems, and, thus, CERN’s operation and assets. However, control systems demand a different approach to security than office systems do.
This poster presents a thorough rule-set to secure CERN’s control systems. Its implementation uses a “Defense-in-Depth” approach based on network segregation, central installation schemes, authentication & authorization, user training, incident response & system recovery, and security auditing

ACKNOWLEDGEMENTS The author would like to thank all his colleagues at CERN involved in the realization of CNIC making it such a success; in particular A. Bland, P. Charrue, I. Deloose, M. Dobson, U. Epting, N. Høimyr, S. Poulsen, and M. Schröder.

REFERENCES

[1] S. Lüders, “Control Systems Under Attack ?”, ICALEPCS, Geneva, October 2005.
[2] U. Epting et al., “Computing and Network Infrastructure for Controls”, ICALEPCS, Geneva, October 2005.
[3] Centre for the Protection of the National Infrastructure (CPNI), “Good Practice Guidelines Parts 1-7”, London, 2006.
[4] I. Deloose, “The Evolution of Managing Windows Computers at CERN”, HEPix, Rome, April 2006.
[5] S. Gysin et al., “Role-Based Access Control for the Accelerator Control System at CERN”; K. Kostro et al., “Role-Based Authorization in Equipment Access at CERN”; A. Petrov et al., “User Authentication for Role-Based Access Control”; and P. Chocula, “Cyber Security in ALICE”, these proceedings.
[6] S. Lüders, “Summary of the Control System Cyber-Security CS2/HEP Workshop”, these proceedings.